AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions and listings of claims in the application:

LISTING OF CLAIMS

Claims

1-43. (cancelled)

44. (New) A method of protecting from modification computer apparatus comprising a plurality of functional modules, wherein the computer apparatus contains or is in communication with a trusted device adapted to respond to a user in a trusted manner, the method comprising:

storing a module configuration of the computer apparatus providing an identification of each functional module in the computer apparatus;

the trusted device performing a cryptographic identification process for modules with a cryptographic identity to identify them and thereby determine an actual module configuration;

the trusted device comparing the actual module configuration against the stored module configuration; and

the trusted device inhibiting function of the computer apparatus while the actual module configuration does not satisfactorily match the stored module configuration.

45. (New) A method as claimed in claim 44, wherein the stored module configuration is held separately from the computing apparatus.

46. (New) A method as claimed in claim 44, wherein the stored module configuration is stored such that it is accessible only by a cryptographic authentication process.

47. (New) A method as claimed in claim 44, wherein the trusted device is adapted to communicate securely with the stored module configuration.

48. (New) A method as claimed in claim 47, wherein the stored module configuration is stored in a security token.

49. (New) A method as claimed in claim 48, wherein the security token is a smart card.

50. (New) A method as claimed in claim 44, wherein the step of checking of the actual module configuration comprises a cryptographic identification process for modules with a cryptographic identity.

51. (New) A method as claimed in claim 48, wherein a stored module configuration is held by a remote module validation authority and the remote validation authority provides a service allowing a replacement security token to be provided if a security token is lost or stolen.

52. (New) Computer apparatus adapted for protection against modification, the computer apparatus comprising a plurality of functional modules, one of said modules being a trusted device adapted to respond to a user in a trusted manner, the computer apparatus having a module configuration providing an identification of each functional module in the computer apparatus, wherein the trusted device is adapted to compare a module configuration of the computer apparatus against a stored module configuration by performing a cryptographic identification process for modules with a cryptographic identity to determine an actual module configuration and to compare the actual module configuration against the stored module configuration

53. (New) Computer apparatus as claimed in claim 52, wherein the stored module configuration is held separately from the computing apparatus and wherein the computer apparatus is adapted to obtain the stored module configuration by a cryptographic authentication process.

54. (New) A security token adapted to hold a stored module configuration of modules in a computer apparatus, the stored model configuration providing providing an identification of each functional module in the computer apparatus as validly formed, and adapted to provide the stored module configuration to the computer apparatus to allow comparison between an actual module configuration of the computer apparatus and the stored module configuration.

55. (New) A security token as claimed in claim 54, wherein the stored module configuration is stored in an encrypted form.

56. (New) A security token as claimed in claim 54, wherein the security token is a smart card.

57. (New) A method of protecting from modification computer apparatus comprising a plurality of functional modules by monitoring the configuration of functional modules within the computer apparatus, the method comprising:

storing a module configuration of the computer apparatus, the module configuration being an identification of each functional module in the computer apparatus as validly formed, on a security token removably attachable to the computer apparatus; and

checking the actual module configuration against the stored module configuration, and inhibiting function of the computer apparatus if the actual module configuration does not satisfactorily match the stored module configuration.

58. (New) A method as claimed in claim 57, wherein the stored module configuration is stored such that it is accessible only by a cryptographic authentication process.

59. (New) A method as claimed in claim 58, wherein the computer apparatus contains or is in communication with a trusted device adapted to respond to a user in a trusted manner and the trusted device is adapted to perform the step of checking the actual module configuration against the stored module configuration.

60. (New) A method as claimed in claim 59, wherein the trusted device is adapted to communicate securely with the security token.

61. (New) A method as claimed in claim 57, wherein the security token is a smart card.

62. (New) A method as claimed in claim 57, wherein the stored module configuration is also held by a remote module validation authority.

63. (New) A method as claimed in claim 62, wherein the step of checking the actual module configuration against the stored module configuration involves use of the stored module configuration held by the remote module validation authority.

64. (New) A method as claimed in claim 62, wherein the remote validation authority provides a service allowing a replacement security token to be provided if a security token is lost or stolen.

* * *